APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/443,204	11/18/1999	JOHN EDWARD FETKOVICH	EN998146	6903

7590   09/25/2003

KEVIN P RADIGAN ESQ
HESLIN & ROTHENBERG PC
5 COLUMBIA CIRCLE
ALBANY, NY 122035160

EXAMINER
SANTOS, PATRICK J D

ART UNIT	PAPER NUMBER
2171	

DATE MAILED: 09/25/2003

3

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*18 November 1999*</u> .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*1-38*</u> is/are pending in the application.

 4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*1-38*</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

 If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

 a)☐ All b)☐ Some * c)☐ None of:

 1.☐ Certified copies of the priority documents have been received.

 2.☐ Certified copies of the priority documents have been received in Application No. _____ .

 3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

 * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

 a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2</u> .

4)☐ Interview Summary (PTO-413) Paper No(s). _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____ .

DETAILED ACTION

Specification

1.   The disclosure is objected to because of the following informalities: the word

"thresholds" is misspelled (page 8, line 28); and the phrase "packetized elementary system"

should read, "packetized elementary stream" (page 18, lines 18-19). Regarding the latter, the

specification wished to further clarify the acronym "PES" within the context of the MPEG

specifications. Within the MPEG specifications, PES is an acronym for "packetized elementary

stream" rather than "packetized elementary system." Appropriate correction is required.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

3.   Claims 1-26, 35, and 38 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

4.   Claims 1-26 recite the limitation "decryption unit" (claim 1, lines 4 and 14-15; claim 14,

lines 4 and 11). There is insufficient antecedent basis for this limitation in the claim. It is not

clear from the claim if the "decryption unit" is a part of the invention or if it is simply an item

that is interacted with by the invention.

5.   Claims 8, 24, and 35 recite the limitation that a stream of compressed data, "**can**

comprise a stream of one of MPEG encoded video data, MPEG encoded audio data, and Dolby

AC-3 audio data" (claim 8, lines 2-3; claim 24, lines 1-4; claim 35, lines 2-4). The word "can" is

indefinite as it implies that the recited formats are incidental rather than necessary to the

operation of the disclosed invention.

6.   Claims 3, 11, 25, and 38 recite the limitation that an "encryption parameter comprises **at**

least some" of a number of parameter types (claim 3, line 2; claim 11, line 3; claim 25, line 3;

and claim 38, line 3). The phrase "at least some" is indefinite as it is non-specific as to what

minimal number constitutes "some." For example, regardless if the number one or more

constituted "some" then claim 3 would be in conflict with claim 2.   Thus the public would not

be able to determine from claims 3, 25, and 38 the where one might infringe.

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8.   Claims 1, 2, 5-8, 12-19, 26 and 27 are rejected under 35 U.S.C. 102(b) as being

anticipated by U.S. Patent No. 5,412,730 issued to Jones (Jones '730).

9.   Regarding Claim 1, Jones '730 teaches corresponding limitations, specifically a method

for protecting a stream of data to be transferred between an encryption unit and a decryption unit

(column 12, lines 25-27; Jones '730), said method comprising:

-       encrypting the stream of data at a said encryption unit for transferring of said

        encrypted stream of data from said encryption unit to said decryption unit

        (column 12, lines 38-39; Jones '730);

-       dynamically varying said encrypting of said stream of data at said encryption

        unit by changing at least one encryption parameter and signaling said change in

        encryption parameter to said decryption unit, said dynamically varying of said at

        least one encryption parameter being responsive to occurrence of a predefined

        condition in said stream of data (column 12, lines 32-37 and column 12, lines

        40-49; Jones '730); and

-       decrypting said encrypted data at the decryption unit, said decrypting accounting

        for said dynamic varying of said encrypting by said encryption unit using said

        changed encryption parameter (column 12, lines 50-51; Jones '730).

10.   The preferred embodiment of Jones '730 discloses an invention in which "means are

employed at both the transmitting and receiving stations to monitor the flow of transmitted data

and to advance the random number generator each time the transmitted data satisfies a

predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the

change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes

dynamic variance. Thus Jones '730 teaches all the limitations of Claim 1.

11.   Regarding Claim 2, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 1 described above, plus specifying at least one encryption parameter that

comprises "at least one of an encryption key, an encryption granularity, an encryption density

scale, an encryption density, an encryption delay, an encryption key update variable, and an

encryption key update data trigger" (column 12, lines 32-37 and column 12, lines 40-49; Jones

'730). Jones '730 teaches the varying of the encryption key. Since this encryption key, which is

varied, is one of the enumerated parameters, this constitutes varying at least one of the

parameters enumerated in Claim 2. Thus Jones '730 teaches all the limitations of Claim 2.

12.   Regarding Claim 5, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 1 described above, plus specifying that "dynamically varying said

encryption parameter based on passage of a predefined number of units of physical data or

passage of a predefined number of conceptual units of data" (column 12, lines 35-37 and

column 12, lines 48-49; Jones '730). Jones '730 teaches use of a block counter to measure the

data stream in order to determine when to vary the cryptographic key used to encrypt and decrypt

the data stream (column 3, lines 33-36 and column 3, lines 64-68; Jones '730). Thus Jones '730

teaches all the limitations of Claim 5.

13.   Regarding Claim 6, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 5 described above, plus specifying that the "encryption parameter comprises

an encryption key" (column 8, lines 26-36; Jones '730). Thus Jones '730 teaches all the

limitations of Claim 6.

14.   Regarding Claim 7, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 1 described above, plus specifying that the "stream of data comprises a

stream a compressed data, and wherein said method further comprises decompressing said

compressed data after said decrypting of said encrypted data by said decrypting unit" (column 2,

line 29; column 8, line 5, and column 8, lines 16-22; Jones '730). Thus Jones '730 teaches all

the limitations of Claim 7.

15.   Regarding Claim 8, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 7 described above, plus specifying that, "said stream of compressed data can

comprise one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio

data" (column 3, lines 12-16; Jones '730). In fact, the method of Jones '730 is independent of

the format of the data to be transmitted. Furthermore, there are no non-obvious consequences of

choosing to carry MPEG or AC-3 data. Thus Jones '730 teaches all the limitations of Claim 8.

16.   Regarding Claim 12, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 1 described above, plus specifying "said encrypting comprises encrypting

multiple portions of said data stream and wherein said dynamically varying comprises

dynamically varying said encrypting of said multiple portions of said data stream by changing

said at least one encryption parameter for each portion of said multiple portions" (column 3, lines

19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block

counter and using a predetermined length as the criteria on when to change the encryption key.

The length of bit stream delineated by the block counter constitutes a portion of the bit stream

and varying the encryption key constitutes changing at least one encryption parameter. Thus

Jones '730 teaches all the limitations of Claim 12.

17.   Regarding Claim 13, Jones '730 teaches corresponding limitations, specifically all the

limitations of Claim 1 described above, plus specifying, "dynamically varying said at least one

encryption parameter responsive to passage of a predefined number of data bits in said stream of data or alternatively, responsive to passage of a predefined number of data units in said stream of data wherein said data units comprise at least one of a program, a sequence, a group of pictures, a slice, or a macroblock" (column 3, lines 19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block counter and using a predetermined length as the criteria on when to change the encryption key. Varying the encryption key constitutes changing at least one encryption parameter. Furthermore, Jones '730 states that, "Advantageously, the block counter may simply count the number of bytes, words or blocks of data being transmitted ..." (column 3, lines 19-22; Jones '730). In the case of MPEG encoding, an implementer who wished to identify such an advantageous block of data would choose MPEG specific data lengths which include items such as a slice or a macroblock as enumerated in Claim 13. Thus Jones '730 teaches all the limitations of Claim 13.

18.   Regarding Claim 14, Jones '730 teaches all the limitations of the claim using a similar argument as provided for Claim 1 above. Specifically, Jones '730 teaches a system that encrypts (column 12, lines 38-39; Jones '730) and decrypts (column 12, lines 50-51; Jones '730) data while varying an encryption parameter (column 12, lines 32-37 and column 12, lines 40-49; Jones '730). In the disclosed embodiment, the varying encryption parameter is an encryption key. Thus, Jones '730 teaches all the limitations of Claim 14.

19.   Regarding Claim 15, Jones '730 teaches all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying of an encryption key (column 8, lines 26-36; Jones '730) using a similar argument as provided for Claim 6 above. Thus, Jones '730 teaches all the limitations of Claim 15.

20.   Regarding Claim 16, Jones '730 teaches all the limitations of Claim 15 as described

above. Furthermore, Jones '730 teaches the disclosed invention applied to digital data (column

3, lines 13-16; Jones '730). Thus, Jones '730 teaches all the limitations of Claim 16.

21.   Regarding Claim 17, Jones '730 teaches all the limitations of Claim 14 as described

above. Furthermore, Jones '730 teaches varying an encryption parameter according to the

passage of bits (column 3, lines 16-25; Jones '730) using a similar argument as provided for

Claim 5. Thus, Jones '730 teaches all the limitations of Claim 17.

22.   Regarding Claim 18, Jones '730 teaches all the limitations of Claim 17 as described

above. Furthermore, Jones '730 teaches encrypting multiple portions of a bit stream (column 3,

lines 19-25; Jones '730) using similar argument as provided for Claim 12 above. Thus, Jones

'730 teaches all limitations of Claim 17.

23.   Regarding Claim 19 Jones '730 teaches all the limitations of Claim 14 as described

above. Furthermore, Jones '730 teaches varying at least one encryption parameter (column 12,

lines 32-37 and column 12, lines 40-49; Jones '730) using a similar argument as provided for

Claim 2 above. Thus, Jones '730 teaches all the limitations of Claim 19.

24.   Regarding Claim 26, Jones '730 teaches all the limitations of Claim 14 as described

above. Furthermore, Jones '730 teaches the additional limitation of Claim 26, that an encryption

parameter be varied for a block of data (column 3, lines 19-25; Jones '730) using a similar

argument as provided for Claim 13 above. Thus Jones '730 teaches all the limitations of Claim

26.

25.   Regarding Claim 27, Jones '730 teaches corresponding limitations, specifically a system

for protecting a stream of data to be transferred between a sender and a receiver (column 1, lines

37-42; Jones '730), said system comprising:

-       an encryption unit disposed at said sender for encrypting the stream of data prior

        to transfer to said receiver, said encryption unit being adapted to dynamically

        vary encrypting of the stream of data by changing at least one encryption

        parameter based on an occurrence of a predefined condition in said data stream

        and signaling said change in encryption parameter to said receiver (column 12,

        lines 38-39; column 12, lines 32-37; and column 12, lines 40-49; Jones '730);

        and

-       a decryption unit disposed at said receiver for decrypting said encrypted data,

        said decryption unit being adapted to receive said changed encryption parameter

        to account for said dynamic varying of said encrypting by said encryption unit

        using said changed encryption parameter (column 12, lines 50-51; Jones '730).

26.   The preferred embodiment of Jones '730 discloses an invention in which "means are

employed at both the transmitting and receiving stations to monitor the flow of transmitted data

and to advance the random number generator each time the transmitted data satisfies a

predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the

change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes

dynamic variance of at least one encryption parameter. Thus Jones '730 teaches all the

limitations of Claim 27.

27.   Claim 28 is rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No.

5,719,937 issued to Warren et al. (Warren '937).

28.   Regarding Claim 28, Warren '937 teaches corresponding limitations, specifically a

program storage device readable by a machine, tangibly embodying at least one program of

instructions executable by the machine to perform a method for protecting a stream of data to be

transferred between an encryption unit and a decryption unit (column 3, lines 42-47; column 6;

lines 28-36; Warren '937), comprising;

-        encrypting the stream of data at said encryption unit for transfer thereof to said

         decryption unit (column 3, line 65 to column 4, line 13; Warren '937);

-        dynamically varying said encrypting of said stream of data at said encryption

         unit by changing an encryption parameter and signaling said change in

         encryption parameter and signaling said change in encryption parameter to said

         decryption unit, wherein said dynamically varying of said encryption parameter

         is responsive to occurrence of a predefined condition in said stream of data

         (column 4, lines 6-12; Warren '937); and

-        decrypting said encrypted data at the decryption unit, said decrypting accounting

         for said dynamic varying of said encrypting by said encryption unit using said

         changed encryption parameter (column 6, line 36 to column 7, line 45 ; Warren

         '937).

29.   The preferred embodiment of Warren '937 is to embed tags that hold metadata that

determine mode of encryption, and may be encoded in real-time (column 4, line 8; Warren '937).

In the disclosed example, the tags can specify a number of ways to vary encryption in a bit

stream (column 5, lines 28-36; Warren '937). Furthermore, the decryptor works in a

complementary way. Finally, the data can be persisted in media such as a DVD or CD (column

6, lines 27-37; Warren '937) but may apply to any compatible storage media. Thus Warren '937

teaches all the limitations of Claim 28.

30.   Claims 1, 13, 14, and 26 are rejected under 35 U.S.C. 102(a) as being anticipated by U.S.

Patent No. 5,991,403 issued to Aucsmith et al. (Aucsmith '403).

31.   Regarding Claims 1 and 13, Aucsmith '403 teaches corresponding limitations,

specifically all the limitations of Claim 1: encrypting data (column 4, lines 55-65; Aucsmith

'403), varying an encryption parameter (column 2, lines 28-30; Aucsmith '403), and decrypting

the data (column 4, line 66 to column 5, line 8; Aucsmith '403). Furthermore it specifies the

additional limitation of Claim 13: "dynamically varying said at least one encryption parameter

responsive to passage of a predefined number of data bits in said stream of data or alternatively,

responsive to passage of a predefined number of data units in said stream of data wherein said

data units comprise at least one of a program, a sequence, a group of pictures, a slice, or a

macroblock" (column 2, lines 28-30; Aucsmith '403).

32.   In the preferred embodiment, the parameter being varied is an encryption key and the

data unit to be encrypted is a group of pictures (GOP) (column 2, lines 28-30; Aucsmith '403).

Thus Aucsmith '403 teaches all the limitations of Claims 1 and 13.

33.   Regarding Claim 26, Aucsmith '403 teaches corresponding limitations, specifically all

the limitations of Claim 14: varying an encryption parameter (column 2, lines 28-30; Aucsmith

'403), and decrypting the data (column 4, line 66 to column 5, line 8; Aucsmith '403). Aucsmith

'403 also teaches the additional limitation of Claim 26 on the same basis as described in the

discussion on Claim 13 above: the varying parameter is an encryption key and the data unit is a

GOP (column 2, lines 28-30; Aucsmith '403). Thus Aucsmith '403 teaches all the limitations of

Claims 14 and 26.

Claim Rejections - 35 USC § 103

34.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

35.   Claims 3, 9-11, 20, and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Jones '730 in view of U.S. Patent No. 5,805,700 issued to Nardone et al. (Nardone '700)

and in further view of U.S. Patent No. 5,933,501 issued to Leppek (Leppek '501).

36.   Regarding Claim 3, Jones '730 teaches all the limitations of Claim 2 as described above.

Jones '730 does not teach varying the following multiple encryption parameters: "an encryption

key, an encryption granularity, an encryption density scale, an encryption density, an encryption

delay, an encryption key update variable, and an encryption key update data trigger"

simultaneously, and furthermore only explicitly teaches varying the encryption key, update

variable, and trigger.

37.   Nardone '700, explicitly teaches encrypting a bit stream taking into account encryption

granularity, density, and delay (column 3, line 65 to column 4, line 13; Nardone '700).

Furthermore, Nardone '700 teaches selectively encrypting a bit stream rather than encrypting the

entire bit stream (column 3, line 65 to column 4 line 13; Nardone '700). Nardone '700 does not

explicitly teach combining with other encryption algorithms.

38.   Leppek '501 teaches varying arbitrary encryption schemes in order to encrypt a bit

stream.

39.   To incorporate the variance of encryption key data as taught by Jones '730, the

encryption granularity and density data as taught by Nardone '700, in addition to any other

arbitrary encryption scheme, using the method taught by Leppek '501, would have been obvious

to a person having ordinary skill in the art at the time of the invention as the combination of the

same is necessary and explicitly taught therein as will be demonstrated below.

40.   The motivation to vary encryption schemes on a bit stream and not just to use the Jones

'730 encryption key variance method, is suggested by Leppek '501 teaching that "a fundamental

characteristic of essentially all encryption operators or algorithms is the fact that, given enough

resources, almost any encryption algorithm can be broken. This, coupled with the fact that each

encryption algorithm has a 'footprint', which is discernable in the scrambled data by a

sophisticated data communications analyst, means that no data communication can be guaranteed

as secure" (column 1, lines 54-60; Leppek '501). In other words, using the same encryption

scheme on a continuous bit stream will eventually provide a statistically significant amount of

data for a hacker to break the encryption scheme. Thus Leppek '501 discloses an invention that,

"combines selected ones of plurality of different encryption operators" (column 1, lines 65-67;

Leppek '501). Furthermore he goes on to teach, "The encryption routines ... need not be any

particular type of encryption algorithm, and may be conventional encrypting operators, such as

PGP, DES..." (column 4, lines 13-17; Leppek '501). Thus Leppek '501 teaches necessity for an

implementer using the Jones '730 encryption key variance method, to vary the encryption

scheme itself in order to reduce the cryptographic footprint of the bit stream.

41.   The motivation to choose the Nardone '700 granularity/density/delay variance method as

an additional encrypting scheme required by the Jones '730/Leppek '501 combination is

suggested by Nardone '700 teaching, "Experience has shown that the decryption and

decompression of a fully encrypted MPEG compressed movie can consume as much as 30% of

the available processor cycles, even with the latest high performance processors" (column 1,

lines 32-38; Nardone '700). An implementer who wished to apply the Jones '730/Leppek '501

combination to MPEG data in order to take advantage of the MPEG market, would be motivated

to choose an encryption algorithm that was not computationally intensive. In fact, Nardone '700

goes on to teach an approach, in which, "a fraction of the BTUs (Basic Transfer Units) ... are

encrypted ...; only a few percent of the processor cycles required by the total encryption

approach for decryption will be required to decrypt and render the {CVD+} (the encrypted bit

stream)..." (column 3, line 65 to column 4 line 13; Nardone '700). Thus, Nardone '700 teaches

the necessity for an implementer using the Jones '730/Leppek '501 combination to use the

Nardone '700 granularity/density/delay variance method as an alternate for the Jones '730

encryption key variance method.

42.   The motivation to use the Nardone '700 granularity/density/delay variance method with

the Jones '730 encryption key variance method in combination, in the context of reducing

cryptographic footprint as taught by Leppek '501 is also suggested by the Nardone '700 teaching

to selectively encrypt the bit stream. As described above. Nardone '700 teaches that one can

approximate bit stream degradation achieved by total encryption, by partially encrypting the bit

stream, and one would further achieve the benefit of requiring less processor cycles. Thus an

implementer would be motivated to use the Jones '730 encryption key variance method to

selectively encrypt the bit stream rather than the entire bit stream as taught by Nardone '700.

Thus Nardone '700 teaches the necessity for an implementer using the Jones '730/Leppek '501

combination to use the Nardone '700 granularity/density/delay variance method not only as an

alternate for the Jones '730 encryption key variance method but also in conjunction with each

other.

43.   In summary, since it would have been necessary for an implementer using the Jones '730

encryption key variance method to reduce cryptographic footprint by using the method of

Leppek '501; and since it would have been necessary for an implementer to choose a low

processing overhead encryption method such as the Nardone '700 granularity/density/delay

scheme as an alternate encryption algorithm in order to efficiently encrypt multimedia data; and

since furthermore it would have been necessary to use the Nardone '700

granularity/density/delay scheme in conjunction with the Jones '730 encryption key variance

method in order to have the Jones '730 method itself be efficient for encrypting multimedia data;

it would have been necessary and obvious to a person having ordinary skill in the art to combine

the teachings of Jones '730, Nardone '700, and Leppek '501 as described above. Thus Claim 3

is rejected under 35 USC 103(a).

44.   Regarding Claim 9, Jones '730 teaches all the limitations of Claim 1 as described above,

including the varying of an encryption key. However, Jones '730 does not teach a "plurality of

encryption parameters being employed by said encrypting and wherein said changed encryption

parameter of said dynamically varying comprises one encryption parameter of said plurality of

encryption parameters." Furthermore, Jones '730 does not teach "initializing a plurality of encryption parameters based on sensitivity of said stream of data."

45.   Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "initializing a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

46.   Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700).

47.   To incorporate the variance of encryption key data as taught by Jones '730, the encryption granularity and density data as taught by Nardone '700, in addition to any other arbitrary encryption scheme, using the method taught by Leppek '501, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as described above. Furthermore, it would have been obvious and necessary to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700 as will be demonstrated below.

48.   The motivation to combine the Jones '730 / Nardone '700 / Leppek '501 in order to provide for "plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption

parameter of said plurality of encryption parameters" is the same motivation as described in Claim 3.

49.   The motivation to combine the "initializing a plurality of encryption parameters based on sensitivity of said stream of data" as taught by Leppek '501 into the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that the Leppek '501 scheme delegates actual encryption to other algorithms and these algorithms inherently require initialization. Leppek '501 describes his disclosed invention as a "virtual encryption scheme" in which "the overall encryption operator itself does not actually perform any encrypting of the data. Instead, it assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence ..." (column 2, lines 6-13; Leppek '501). Thus the Leppek '501 invention would have to delegate to other encryption methods in order to actually encrypt the bit stream. Both the Jones '730 and Nardone '700, which are used in combination with Leppek '501 require initialization choices to be made (column 3; lines 26-40; Jones '730 and column 1, lines 50-59; Nardone '700). Thus in order to be used in combination with the invention of Leppek '501, the Jones '730 and Nardone '700 algorithms must be initialized. Furthermore, Nardone '700 teaches a motivation to set encryption granularity and density in order to reduce processing cycles (column 3, line 65 to column 4 line 13; Nardone '700). From this it is inherent that the initialization values should be set based on a tradeoff between processing overhead and adequate encryption. Thus it would have been obvious to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700. Thus Claim 9 is rejected under 35 USC 103(a).

50.   Regarding Claim 10, Jones '730 teaches all the limitations of Claim 1 as described above.

Jones '730 does not explicitly teach the setting and varying of parameters, nor does it explicitly

teach the use of MPEG compressed data as the data payload of a bit stream, nor does it explicitly

teach the use of sensitivity of the bit stream for a criterion for setting parameters.

51.   Leppek '501 teaches the use of multiple encryption algorithms as described above.

Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66;

Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

52.   Nardone '700 teaches the varying of granularity and density encryption, specifically only

encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches

"sensitivity of said stream of data" as a criterion for encryption parameter initialization (column

3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment

in which the bit stream is composed of MPEG compliant video data and MPEG compliant audio

data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

53.   The motivation to combine the Jones '730 / Nardone '700 / Leppek '501 in order to

provide for "plurality of encryption parameters for use by said encrypting" is the same

motivation as described in Claim 3.

54.   The motivation to use MPEG compressed data as the payload of the Jones '730 / Nardone

'700 / Leppek '501 in combination would be to make the combination applicable to the large

MPEG market. A practitioner would have been motivated to use MPEG compliant data as the

payload in the Jones '730 / Nardone '700 / Leppek '501 combination. In fact, the motivation to

use the Nardone '700 granularity/density/delay encryption method was motivated by balancing

processing overhead with encryption security in multimedia data.

55.   The motivation to use sensitivity of stream data as a criterion for encryption parameter

initialization in the Jones '730 / Nardone '700 / Leppek '501 combination is the same motivation

as described in Claim 9.

56.   Thus, it would have been necessary and obvious to a person having ordinary skill in the

art to use MPEG compressed data and to use sensitivity of stream data as a criterion for

encryption parameter initialization in the Jones '730 / Nardone '700 / Leppek '501 combination.

Thus Claim 10 is rejected under 35 USC 103(a).

57.   Regarding Claim 11, Jones '730 teaches the limitations of Claim 1 as described above.

Jones '730 does not teach all the limitations of Claim 10. Furthermore, Jones '730 does not

teach the setting of a, "plurality of encryption parameters ... establishing at least some of an

encryption granularity, and initial encryption key, a density scale, a density, an encryption delay,

and a key update data trigger for said stream of MPEG encoded data."

58.   Leppek '501 teaches the use of multiple encryption algorithms as described above.

Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66;

Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

59.   Nardone '700 teaches the varying of granularity and density encryption, specifically only

encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches

"sensitivity of said stream of data" as a criterion for encryption parameter initialization (column

3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment

in which the bit stream is composed of MPEG compliant video data and MPEG compliant audio

data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

60.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to provide

for the setting of "plurality of encryption parameters ... establishing at least some of an

encryption granularity, and initial encryption key, a density scale, a density, an encryption delay,

and a key update data trigger," is described in the discussion regarding Claim 10 above.

61.   The motivation to apply the Jones '730 / Nardone '700 / Leppek '501 combination

method to a "stream of MPEG encoded data" is described in the discussion regarding Claim 3

above.

62.   As such it would have been necessary and obvious to a person having ordinary skill in the

art apply the setting of the enumerated encryption parameters to MPEG encoded data. Thus

Claim 11 is rejected under 35 USC 103(a).

63.   Regarding Claim 20, Jones '730 teaches all the limitations of Claim 19 as described

above. Jones '730 does not teach the setting multiple encryption parameters, including in

combination.

64.   Nardone '700 teaches the setting of a encryption granularity/density/delay and the

selective encoding of a bit stream as described above.

65.   Leppek '501 teaches the rotating among several encryption algorithms as described

above.

66.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to set multiple

encryption parameters is the same as described in the discussion regarding Claim 3. As such, it

would have been necessary and obvious for a person having ordinary skill in the art to modify

Jones '730 to set multiple encryption parameters, including in combination, as described in the

discussion above regarding Claim 3. Thus Claim 20 is rejected under 35 USC 103(a).

67.   Regarding Claim 22, Jones '730 teaches all the limitations of Claim 14 as described

above. However, Jones '730 does not teach setting of multiple parameters based on sensitivity

of the data.

68.   Nardone '700 teaches the setting of a encryption granularity/density/delay and the

selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of

said stream of data" as a criterion for encryption parameter initialization as described above.

69.   Leppek '501 teaches the rotating among several encryption algorithms as described

above.

70.   The motivation combine Jones '730, Nardone '700, and Leppek '501 in order to set of

multiple parameters based on sensitivity of the data is described in the discussion above

regarding Claim 9. As such, it would have been necessary and obvious for a person having

ordinary skill in the art to modify Jones '730 to set multiple parameters based on sensitivity of

data. Thus Claim 22 is rejected under 35 USC 103(a).

71.   Regarding Claim 23, Jones '730 teaches all the limitations of Claim 14 as described

above. Jones '730 does not explicitly teach the additional limitations of Claim 22 which Claim

23 incorporates. Furthermore, Jones '730 does not explicitly teach the use of a decompression

decoder.

72.   Nardone '700 teaches the setting of a encryption granularity/density/delay and the

selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of

said stream of data" as a criterion for encryption parameter initialization as described above.

Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2,

lines 56-66; Nardone '700), which implies an MPEG decoder, which in turn implies a

decompression decoder.

73.   Leppek '501 teaches the rotating among several encryption algorithms as described

above.

74.   The motivation to combine Jones '730 with Nardone '700 and Leppek '501, to set a

plurality of encryption parameters is described in the discussion above regarding Claim 22.

75.   The motivation to combine Jones '730 with Nardone '700 and Leppek '501 in order to

carry compressed data and to use MPEG data is inherent in the the desire to carry MPEG data.

In fact, Nardone '700 explicitly teaches the use of MPEG data. As a result, in order to render the

data, adding an MPEG decoder after encryption is inherent in the Jones '730 / Nardone '700 /

Leppek '501 combination. Since MPEG is inherently a compression standard, addition of the

MPEG decoder constitutes adding a decompression decoder. As such, it would have also been

necessary and obvious for a person having ordinary skill in the art to combine Jones '730 with

Nardone '700 and Leppek '501 not only for the reasons enumerated in the discussion regarding

Claim 22, but also for the benefit of a decompression decoder. Thus Claim 23 is rejected under

35 USC 103(a).

76.   Regarding Claim 24, Jones '730 teaches all the limitations of Claim 14 above. However,

Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 24 incorporates.

Furthermore, Jones '730 does not explicitly teach the use of MPEG, video and audio, and Dolby

AC-3 data for the data payload.

77.   Nardone '700 teaches the setting of a encryption granularity/density/delay and the

selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of

said stream of data" as a criterion for encryption parameter initialization as described above.

Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2,

lines 56-66; Nardone '700), which implies an MPEG decoder.

78.   Leppek '501 teaches the rotating among several encryption algorithms as described

above.

79.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to set a plurality of

encryption parameters and to use compressed data is described in the discussion regarding Claim

23 above.

80.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to use MPEG data

is inherent in the discussion regarding Claim 23 above. The counterexample in the discussion

above on Claim 23 explicitly refers to the Nardone '700 in which MPEG, video and audio, and

Dolby AC-3 data is used for the data payload (column 2, lines 56-66; Nardone '700). Thus it

would have been obvious for a person having ordinary skill in the art to combine Jones '730 /

Nardone '700 / Leppek '501 in order to set multiple encryption parameters, and to use

MPEG/AC-3 multimedia data for a data payload. Thus Claim 24 is rejected under 35 USC

103(a).

81.   Regarding Claim 25, Jones '730 teaches all the limitation of Claim 14 above. However,

Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 25 incorporates.

Furthermore, Jones '730 does not explicitly teach the limitation of initializing a number of

encryption parameters.

82.   Nardone '700 teaches the setting of a encryption granularity/density/delay and the

selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of

said stream of data" as a criterion for encryption parameter initialization as described above.

Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2,

lines 56-66; Nardone '700), which implies an MPEG decoder.

83.   Leppek '501 teaches the rotating among several encryption algorithms as described

above. Leppek '501 also teaches the initialization of encryption parameters as described above.

84.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet the

limitations of Claim 23 is described in the above discussion regarding Claim 23.

85.   The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet

initialize multiple encryption parameters is described in the above discussion regarding Claim

11.

86.   Thus it would have been obvious for a person having ordinary skill in the art to combine

Jones '730 / Nardone '700 / Leppek '501 to meet the limitations of Claim 25. Thus Claim 25 is

rejected under 35 USC 103(a).

87.   Claims 4 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones

'730 in view of Nardone '700 and Leppek '501 and in further view of "Digital Television

Achieves Maturity" by Leonardo Chiariglione, copyrighted 1998 (Chiariglione '98).

88.   Regarding Claim 4, Jones '730 / Nardone '700 / Leppek '501 in combination teach all the

limitations of Claim 3 as described above. Furthermore, Nardone '700 teaches varying

encryption schemes via a policy (column 2, lines 40-46; Nardone '700) and furthermore in a

disclosed embodiment teaches varying the policy dynamically (column 4, lines 23-42; Nardone

'700). However, Jones '730 / Nardone '700 / Leppek '501 do not teach multiplexing in the variance information into the encrypted bit stream.

89.   Chiariglione '98 teaches multiplexing in the variance information into the encrypted bit stream (page 2, line 32 to page 3, line 8, and Figure 1; Chiariglione '98).

90.   To incorporate the multiplexing in of variance information into the encrypted bit stream as taught by Chiariglione '98, to the Jones '730 / Nardone '700 / Leppek '501 combination, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as will be demonstrated below.

91.   The motivation to transmit dynamically varying encryption policy information via the Chiariglione '98 within the context of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that both disclosures are refer to the encryption/decryption of multimedia data. Selectively encrypt a bit stream as taught by Nardone '700 is a direct consequence of handling multimedia data. The Chiariglione '98 teaching discusses the MPEG-2 specification, which discloses use of EMM and ECM messages multiplexed into the bit stream in order to provide access control information dynamically. In order to take advantage of the MPEG market, the inventor would have been motivated to use of EMM and ECM messages multiplexed into the bit stream as taught by the MPEG specification. As such, it would have been necessary and obvious to apply the Chiariglione '98 teaching with the Jones '730 / Nardone '700 / Leppek '501 combination in order to be compliant with the MPEG specification and thus be salable in the MPEG market. Thus Claim 4 is rejected under 35 USC 103(a).

92.   Regarding Claim 21, Jones '730 teaches all the limitations of Claim 14. However, Jones '730 does not teach multiplexing in the encryption parameter in with the bit stream.

93.   However, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination described in the discussion regarding Claim 4 above teaches multiplexing in the encryption parameter in with the bit stream.

94.   It would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to multiplex in the encryption parameter in with the bit stream as described in the discussion above regarding Claim 4. Thus Claim 21 is rejected under 35 USC 103(a).

95.   Claims 29, and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable in view of Jones '730 in view of Warren '937.

96.   Regarding Claims 29 and 32-35, Jones '730 teaches corresponding limitations in all the aforementioned claims with the exception of explicitly teaching a program storage device. Refer to the discussions regarding Claims 2, and 5-8 respectively.

97.   Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) as described in the discussion regarding Claim 28 above.

98.   The motivation to apply the encryption scheme of Jones '730 to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of Jones '730 is suggested by Jones '730, "For increased data security, the encryption key value may be changed frequently to further reduce the

likelihood that an unauthorized party may decipher the data" (column 1, lines 22-25; Jones '730).

Thus an implementer who used the program storage device and copy management method of

Warren '937, who desired to reduce the ability to hack the data would be motivated to add the

encryption method of Jones '730. Thus, Claims 29, 32-35 are rejected under 35 USC 103(a).

99.   Claims 30, and 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Jones '730, Nardone '700, and Leppek '501 in view of Warren '937.

100.   Regarding Claims 30 and 36-38, Jones '730, Nardone '700, and Leppek '501 in

combination teach corresponding limitations in all the aforementioned claims with the exception

of explicitly teaching a program storage device. Refer to the discussions regarding Claims 3, 14,

10, and 11 respectively.

101.   The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 /

Leppek '501 combination to the program storage device of Warren '937 is suggested by Warren

'937, "it would be desirable to provide an electronic copy management scheme for controlling

the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937

discloses one such invention. Furthermore, the motivation to use the method of the Jones '730 /

Nardone '700 / Leppek '501 combination is suggested by Warren '937, "it is assumed that the

source material which is stored on the media is compressed data, and that the media is a laser

disk, compact disk, or DVD" (column 6, lines 28-31; Warren '937). The context of the Warren

'937 invention is that of multimedia data. As discussed above, the Jones '730 / Nardone '700 /

Leppek '501 provides a cryptographic combination motivated to be applied to multimedia data.

Thus a practitioner ordinarily skilled in the art would be motivated to apply the Jones '730 /

Nardone '700 / Leppek '501 method to the program storage device of Warren '937. Thus

Claims 30, and 36-38 are rejected under 35 USC 103(a).

102.   Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones '730,

Nardone '700, Leppek '501, and Chiariglione'98 in view of Warren '937.

103.   Regarding Claim 31, Jones '730, Nardone '700, Leppek '501, and Chiariglione'98 teach

corresponding limitations with the exception of explicitly teaching a program storage device as

described in the discussion regarding Claim 4 above.

104.   Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) as

described in the discussion regarding Claim 28 above.

105.   The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 /

Leppek '501 / Chiariglione '98 combination to the program storage device of Warren '937 is

suggested by Warren '937, "it would be desirable to provide an electronic copy management

scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren

'937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the

method of the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination is

suggested by Warren '937, "it is assumed that the source material which is stored on the media is

compressed data, and that the media is a laser disk, compact disk, or DVD" (column 6, lines 28-

31; Warren '937). The context of the Warren '937 invention is that of multimedia data. As

discussed above, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 provides a

cryptographic combination, including multiplexing encryption data. Thus a practitioner with

ordinary skill in the art would be motivated to apply the Jones '730 / Nardone '700 / Leppek

'501 / Chiariglione '98 method to the program storage device of Warren '937. Thus Claim 31 is

rejected under 35 USC 103(a).

Conclusion

106.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

ISO/IEC JTC1/SC29/WG11 MPEG-2 "Generic Coding of Moving Pictures and

Associated Audio Information." <http://www.chiariglione.org/mpeg/standards/mpeg-2/mpeg-

2.htm>. This document is a quick overview of the MPEG-2 specification, which provides

much motivational material for the encryption of video and audio data. This document

comes from Leonardo Chiariglione's web site. Chiariglione is a key member of the

MPEG standards effort.

"Open Platform Initiative for Multimedia Access (OPIMA) – Call for Proposals for

Technologies." <http://leonardo.telecomitalialab.com/opima/paris/opima_cfp.htm>. This is another

document from Chiariglione on video and audio encryption. As a result of being a call

for proposals for a standards body, provides a detailed description of design issues for the

encryption of video and audio data.

107.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Patrick J Santos whose telephone number is 703-305-0707. The

examiner can normally be reached on M-F 8:00-4:30.

108.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Safet Metjahic can be reached on 703-308-1436. The fax phone number for the

organization where this application or proceeding is assigned is (703) 872-9306.

109.   Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

pjs

SAFET METJAHIC
SUPERVISORY PRIMARY EXAMINER
TECHNOLOGY CENTER 2100